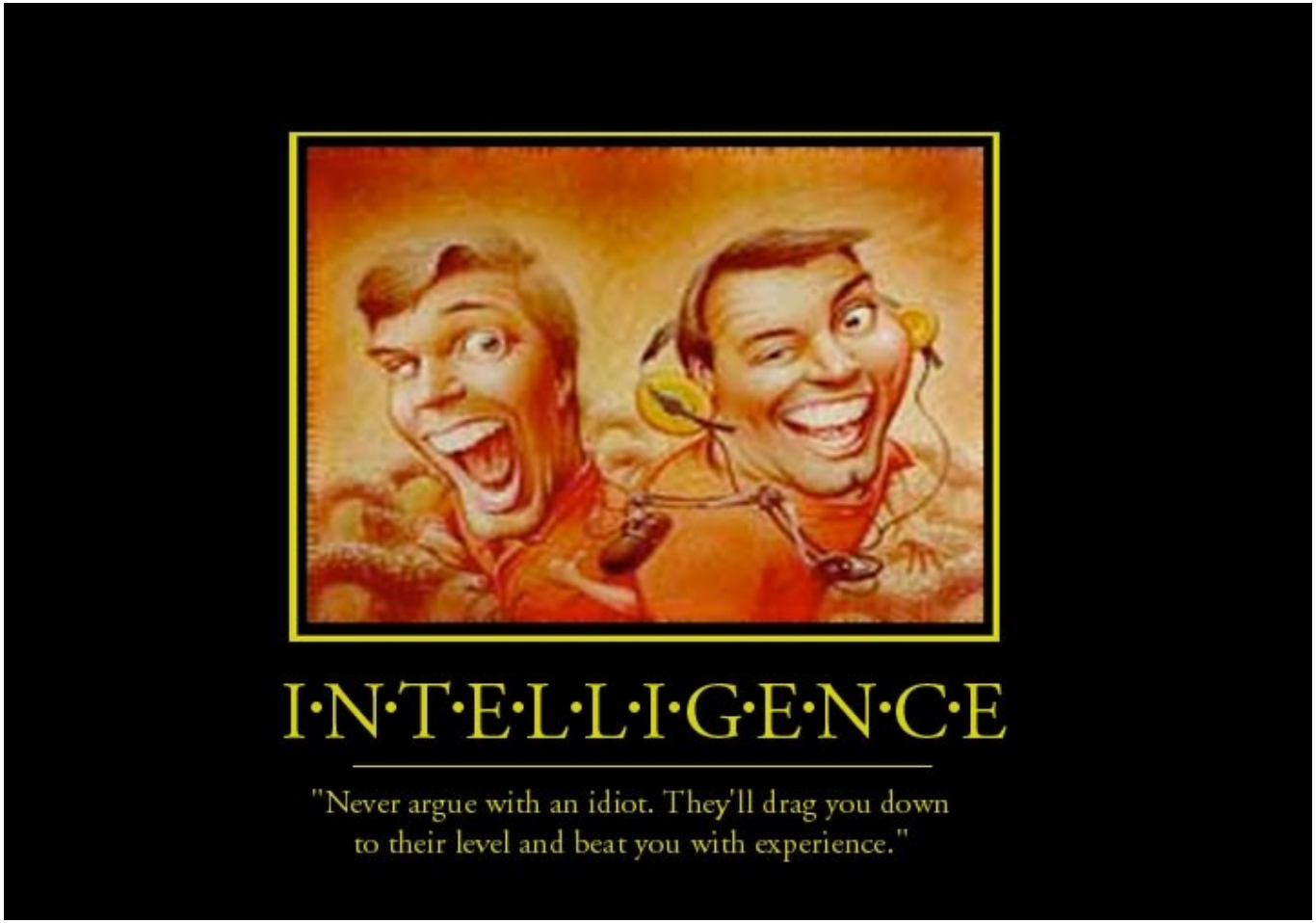
Risk – A Small Agency's Viewpoint

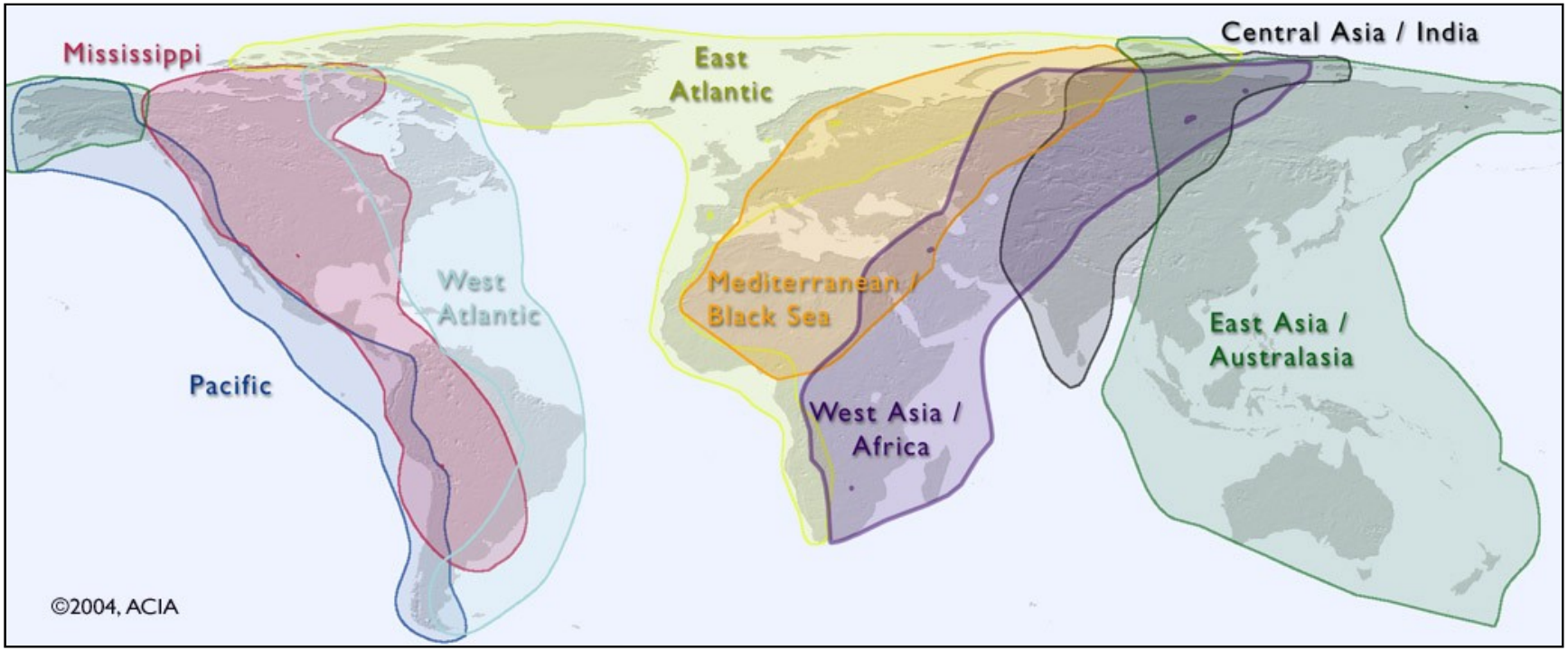
DoD Internal Control Conference

2 December 2005

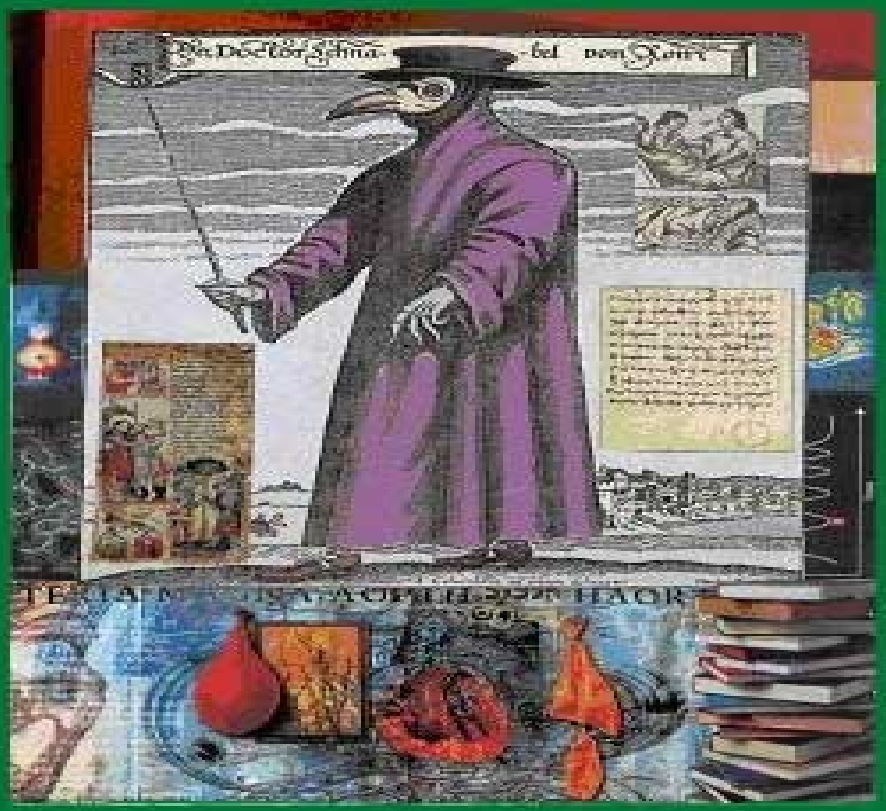
Ken Murphy / DIA ICP Coordinator
Kenneth.Murphy@ dia.mil
703-907-0308

Intelligence Risks



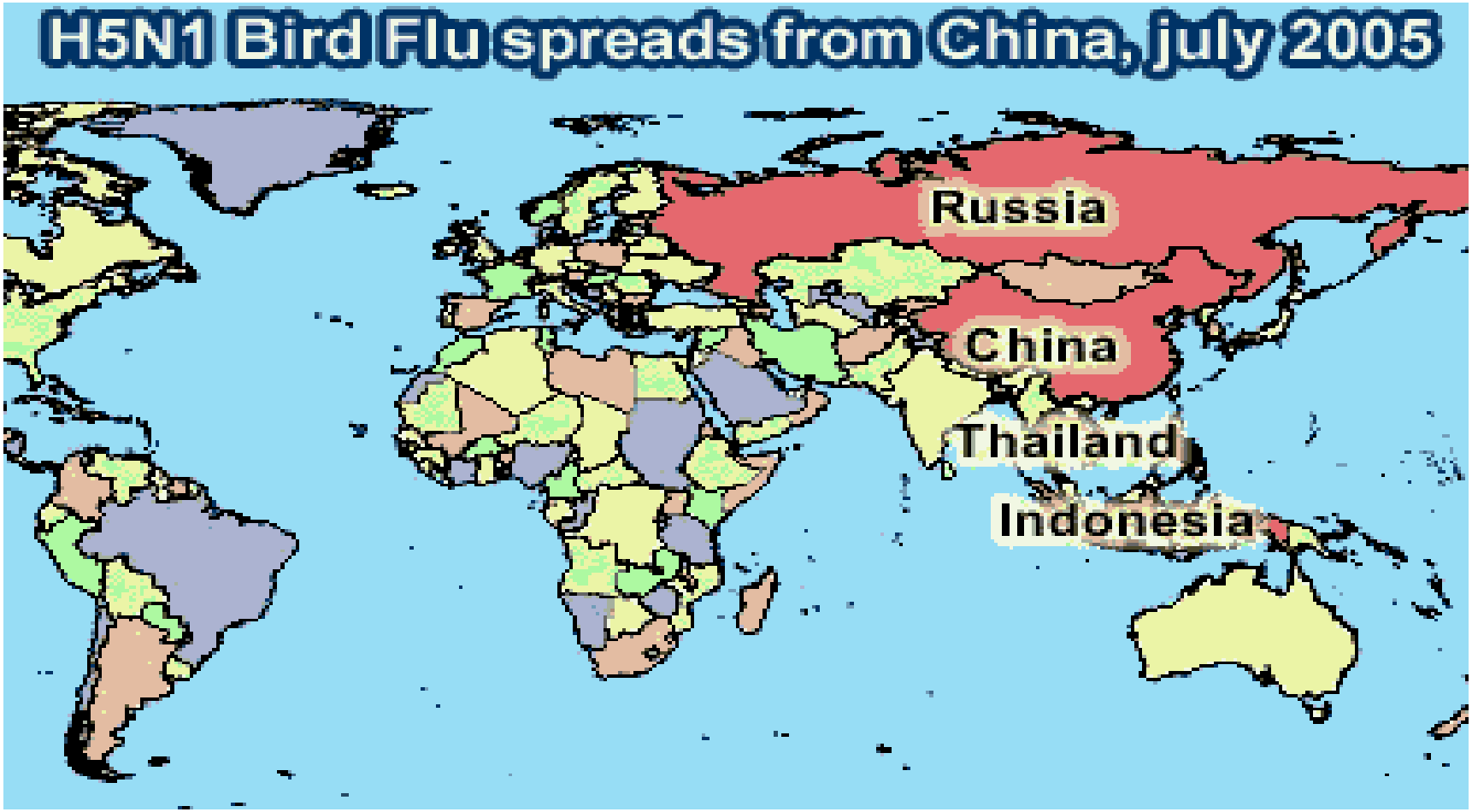

Mississippi
East Atlantic
Central Asia / India
West Atlantic
Mediterranean / Black Sea
East Asia / Australasia
Pacific
West Asia / Africa
©2004, ACIA

Risk Depiction



Risk Response

World at Risk



SOA Assertions

Four Assertions in the Statement of Assurance:

- **An evaluation of controls was done.**
- **Controls are in place.**
- **Controls are operating.**
- **Controls enable achievement of FMFIA objectives.**

FMFIA Objectives

- **Internal control objectives are that the organization, policies, and procedures reasonably ensure:**
  - **Compliance with laws and regulations.**
    - **Obligations and costs are in compliance with applicable law.**
  - **Effective and efficient operations.**
    - **Assets are safeguarded against waste, loss, unauthorized use, and misappropriation.**
  - **Reliable financial reporting.**
    - **Revenues and expenditures are properly recorded and accounted for to permit reliable reports and maintain accountability.**

Assurance

Assurance Concept

Assurance may be absolute or may be reasonable.

With absolute assurance, the result is guaranteed under all circumstances.

With reasonable assurance, the result is an opinion of a likely outcome.

The opinion on the outcome is based on the qualifications of the evaluator, the concealment that occurs with fraud, the use of samples rather than 100% testing, and, the interpreting the results of testing.

As a result of so much judgment used in the evaluation process, the evidence from testing is persuasive, rather than convincing, and the assurance is reasonable, rather than absolute.

Thus the annual assurance states that there is reasonable assurance that management controls are in-place and operating effectively to meet FMFIA objectives.

COSO Risk Management Framework

COMPONENTS

- Internal Environment.
- Objective Setting.
- Event Identification.
- Risk Assessment.
- Risk Response.
- Control Activities.
- Information and Communication.
- Monitoring.

Internal Environment

- Foundation of other components of risk management.
- Management sets a philosophy regarding risk.
- Forms how risk is viewed by entity's personnel.
- Personnel attributes of integrity, ethics, and competence.
- Environmental attributes of structure, authority, human resources.
- Board of Directors is part of the environment.

Objective Setting

- Objectives – what an entity hopes to achieve.
- Entity's reason for being.
- Activity level (program) linked to strategic goals.
- Include measurement criteria.
- Should be basis for assessable units.

Assessable Units

Defined:

- **Any organizational, functional, programmatic, or other subdivision that has a control assigned.**
- **Specific controls for specific responsibilities, and / or general controls for broader responsibilities.**
- **Lowest level where controls are evaluated.**
- **Not only financial – controls ensure objectives are achieved.**
- **Objectives relate to any activity and any resource.**
- **Simply – an assessable unit is anywhere one places a control to ensure that an objective is achieved.**

Event Identification - Risk

- Management identifies potential events affecting an entity's ability to successfully implement strategy and achieve objectives.
- Events with a potentially negative impact represent risks.
- Events with a potentially positive impact represent opportunities.
- Events are an incident or occurrence emanating from internal or external sources that could affect implementation of strategy or achievement of objectives.
- External events – economic, business, natural, political, social, technological.
- Internal events – infrastructure, personnel, process, technology.
- Part of short term and long term forecasting and strategic planning.

Risk Assessment

- To consider the extent to which potential events might impact the achievement of objectives.
  - Entity's ability to initiate, record, process, and report financial data consistent with financial statement assertions.
- Exist, complete, valuation, rights/obligations, disclosure
- Evaluated from two perspectives – likelihood and impact.
  - Likelihood – possibility that the event will occur.
  - High, medium, low.
- Includes consideration of time horizon..
- Impact – effect.
- Control risk – internal control will not prevent or detect.
- Inherent risk – susceptibility to error when controls do not exist.

Categorization

- **Designation of weakness is management judgment based on relative risk.**
- **Adversely affect the organization's ability to meet mission objectives is a reportable condition.**
- **Significant reportable condition that the DOD Component head determines to be significant enough to be reported outside the component is a material weakness.**
- **The decision on whether a weakness is material is a leadership judgment.**

Risk Response

- Risk avoidance, reduction, sharing, and acceptance.
- Costs (objective) and benefits (subjective).
- **Avoidance** – exit activities giving rise to risks – too costly or no change.
- **Reduction** – Reduce likelihood or impact – reduce to risk tolerance – acceptable residual risk.
- **Sharing** – insurance – reduce to risk tolerance – acceptable residual risk.
- **Acceptance** – no action to affect likelihood or impact – inherent risk in line with risk tolerance.

Risk Response

Control Activities

- Control activities ensure management's risk responses are carried out.
- Policies, procedures, techniques, mechanisms to mitigate risk identified during risk assessment and carry out management directives.
- Some control activities are designed specifically for information systems.
- General – structure, policies, and procedures that apply to an agency's overall computer operations.
- Application – structure, policies, and procedures designed to help ensure the completeness, accuracy, authorization and validity of data capture and transaction processing.

Examples of Control Activities

- Top level reviews of actual performance
- Human capital management policies
- Information processing controls
- Functional or activity level reviews
- Physical control over vulnerable assets
- Access restrictions to resources
- Performance measures and indicators
- Accurate and timely recording of transactions
- Segregation of duties
- Proper execution of transactions
- Documentation of transactions
- Accountability records

Information and Communication

- Pertinent information must be identified, captured, and communicated in a form and timeframe that enable personnel to carry out their responsibilities.
- Information is needed at all levels of the organization to identify, assess, and respond to risks and to run the entity and achieve its objectives.
- Historical data allow the entity to track actual performance against targets, plans, and expectations.
- Current data allow an entity to assess its risks at a specific point in time and to remain within established risk tolerances.
- Information is the basis for communications.

Monitoring

- **Monitoring is a process that assesses both the presence and functioning of its components and the quality of their performance over time.**
- **Monitoring can be ongoing or separate.**
- **Ongoing is built into the normal, recurring operating activities of the entity. Ongoing monitoring is performed on a real-time basis, reacts dynamically to changing conditions, and is ingrained in the entity.**
- **Separate evaluations take place after the fact.**
- **Problems are identified more quickly by ongoing monitoring routines.**

COSO Enterprise Risk Management Framework

COMPONENTS

- Internal Environment.
- Objective Setting.
- Event Identification.
- Risk Assessment.
- Risk Response.
- Control Activities.
- Information and Communication.
- Monitoring.

Risk – A Management Judgment